

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of:

Information associated with adedotun_adebogun@yahoo.com,
benshak@yahoo.com, michael.john160@yahoo.com, and
jazz_jassan@yahoo.com that is stored at premises owned,
maintained, controlled, or operated by Oath Holdings Inc.

Case No. 19-978M(NJ)

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment A

over which the Court has jurisdiction pursuant to Title 18, United States Code, Sections 2703 and 2711, there is now concealed:

See Attachment B

The basis for the search under Fed. R. Crim P. 41(c) is:

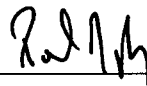
- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of:

18 U.S.C. Sections 1343 (Wire Fraud), 1349 (Attempt and Conspiracy), and 1956 (Money Laundering)

The application is based on these facts: See attached affidavit.

- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Park Jones, IRS CI Special Agent

Printed Name and Title

Sworn to before me and signed in my presence:

Date:

November 25, 2019



Judge's signature

City and State: Milwaukee, Wisconsin

Honorable Nancy Joseph, U.S. Magistrate Judge

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR SEARCH WARRANT**

I, Park J. Jones, having been duly sworn on oath, state as follows:

INTRODUCTION AND BACKGROUND

1. I am employed as a Special Agent with the Internal Revenue Service, Criminal Investigation (IRS-CI) and have been employed since September 2005. My responsibilities as a Special Agent include the investigation of potential criminal violations of the Internal Revenue Code under Title 26 of the United States Code as well as related Title 18 and Title 31 offenses. In my career, I have conducted multiple investigations involving money laundering and have obtained search and seizure warrants for criminal proceeds and property involved in money laundering. In the course of those investigations, I have used various investigative techniques, including undercover operations, reviewing physical and electronic evidence, and obtaining and reviewing financial records. In the course of those investigations, I have also become familiar with techniques that criminals use to conceal the nature, source, location, and ownership of proceeds of crime and to avoid detection by law enforcement of their underlying acts and money laundering activities.

2. Because I am submitting this affidavit for the limited purpose of establishing probable cause for the requested seizure warrant, I have not included in this affidavit every detail I know about this investigation. Rather, I have included only the information necessary to establish probable cause for the requested seizure warrant.

3. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that are stored at premises controlled by Oath Holdings Inc., an email provider headquartered at 701 First Avenue, Sunnyvale, California 94089. The information to be searched is described in the following paragraphs and in Attachment A.

This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Oath Holdings Inc. to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18 U.S.C. Sections 1343, 1349 and 1956 have been committed by Adedotun Adebogun or other unknown persons. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

6. Over the last few years, law enforcement has seen an increase in business email compromise (“BEC”) schemes. A BEC scheme is a form of cybercrime which uses a fraudulent email to obtain funds from an organization or business entity. The scheme typically targets employees in financial roles and with access to entity funds within the victim organization. The fraudulent email will provide false instructions regarding financial transactions in order to defraud the employee into sending money or sensitive personal identifying data to the fraudster’s bank account.

7. St. John XXIII is a religious institution located in Port Washington, Wisconsin, within the Eastern District of Wisconsin. CG Schmidt is a construction management and general contracting firm based in Milwaukee, Wisconsin. St. John XXIII hired CG Schmidt as a contractor to assist with a construction project at St. John XXIII.

8. On or about February 26, 2019, the St. John XXIII accounts payable department received a letter by email attachment from an individual purporting to be have the initials B.N. and purporting to be the Chief Financial Officer of CG Schmidt, requesting the direct deposit/ACH authorization form to update CG Schmidt's banking information.

9. A few days after the receipt of that letter, an individual having the initials T.A., who purported to be an employee of CG Schmidt, contacted an employee at St. John XXIII via phone. T.A. wanted to confirm receipt of the letter and inquired about future payments. T.A. then sent the employee at St. John XXIII a follow up email.

10. The emails to St. John XXIII were sent from the email address XXXXXerg@cgschmidtinc.com, while CG Schmidt's actual email domain is XXXXX@cgschmidt.com.

11. Based upon the phone conversations and emails from XXXXXerg@cgschmidtinc.com, the St. John XXIII employee changed the bank account information for payments made to CG Schmidt to a BBVA Compass Bank account with an account number ending in 8886 ("BBVA 8886").

12. On or about March 4, 2019, the St. John XXIII employee initiated a wire transfer of \$510,058.97 from St. John XXIII's bank account at Port Washington State Bank to BBVA 8886 as payment for construction services performed by CG Schmidt.

13. I reviewed the BBVA Compass Bank records associated with BBVA 8886. The account was opened on June 11, 2018, in the name of MJT Ventures, with the owner and authorized signor listed as Malcolm Tayloy ("Tayloy").

14. Tayloy used a British passport as an identifying document to open the account. A search of border entry records did not reveal any entries of Tayloy into the United States. It is believed the Tayloy passport is fraudulent.

15. After the March 4, 2019 St. John XXIII wire transfer of \$510,058.97 to BBVA 8886, the funds in the BBVA account were transferred to five different bank accounts. Two of the fund transfers were to accounts at JP Morgan. The transfers were conducted on March 7 and 8, 2019, in the amounts of \$97,810.90 and \$64,700.00, respectively. The March 7 transfer was to a JP Morgan account with an account number ending in 1581 ("JPM 1581"), held in the name of David James d/b/a Aris Ventures. The March 8, 2019 transfer was to a JP Morgan account with an account number ending in 8736 ("JPM 8736"), held in the name of Michael John.

16. I reviewed bank records associated with JPM 1581. The account was opened in Phoenix, Arizona on December 20, 2018, in the name of David James d/b/a Aris Ventures. The only authorized signor on the account is James. The email address associated with the account was jazz_jassan@yahoo.com. James presented a Nigerian passport to open JPM 1581.

17. I reviewed bank records associated with JPM 8736. The account was opened in Richardson, Texas on February 7, 2019, in the name of Michael John. The only authorized signor on the account is John. The email address associated with the account was michael.john160@yahoo.com. John presented a Great Britain passport to open JPM 8736.

18. From March 8 thru March 12, 2019, the funds in account JPM 1581 were depleted with four cash withdrawals totaling \$28,700 and a wire transfer of \$68,460 to a business located in Nigeria.

19. On March 11, 2019, the funds in account JPM 8736 were depleted with three cash withdrawals totaling \$23,000 and a wire transfer of \$40,000 to a business located in Uganda.

20. On March 13, 2019, Port Washington State Bank contacted an employee of St. John XXIII and informed that employee that the wire transfer to BBVA 8886 was fraudulent because the funds were transferred to an account titled MJT Ventures rather than to CG Schmidt.

21. Later that day, the fraud department at BBVA Compass Bank then informed the St. John XXIII employee that the \$510,058.97 in funds that St. John XXIII had wire transferred to BBVA 8886 had already been transferred out of BBVA 8886.

22. A representative from CG Schmidt confirmed the following:

- a. No one had permission to use CG Schmidt's logo or letterhead to request that CG Schmidt's bank account be changed;
- b. CG Schmidt is not affiliated with BBVA 8886;
- c. The emails from XXXXXerg@cgschmidtinc.com were fraudulent;
- d. The CG Schmidt CFO listed on the February 26, 2019 letter has not been employed with the company for the last 10 years; and
- e. The employee name on the emails, with the initials T.A., has never been employed at CG Schmidt.

23. Your affiant obtained the Internet Protocol ("IP") address used to log into the JP Morgan bank accounts remotely. An IP address is numerical label assigned to each device connected to a computer network that uses IP for communication. The IP address for each device is assigned by an Internet Service Provider ("ISP").

24. The IP address used to log into JPM 8736 was xx.xxx.xx.69. I obtained the subscriber information associated with this IP Address from the ISP. The subscriber was listed as an individual named Koyode Jackson located at 3950 Spring Valley Road #921 in Farmers Branch,

Texas. Other identifying information associated with the subscriber account was an email address of benshak@yahoo.com and a phone number of 682-347-2424. The IP address of xx.xxx.xx.69 was used at this address for the period of December 28, 2018 thru June 29, 2019.

25. I attempted to identify Jackson using the address and phone number provided by the provider. I could not identify Jackson based on the address and phone number provided. It appears Jackson is a fictitious name.

26. I then conducted a FinCEN search using the address and email address provided. The search of the address resulted in the identification of a Currency Transaction Report "CTR" filed by Wells Fargo Bank on an individual named Adedotun Adebogun ("Adebogun"). The CTR was filed on April 10, 2019 for a cash deposit of \$11,800. The phone number associated with the account was 682-347-2424. This is the same phone number associated with the subscriber account of Koyode Jackson. The email address associated with the Wells Fargo bank account was adedotun_adebogun@yahoo.com.

27. I obtained a Texas driver's license photo of Adebogun. I then obtained digital photo snapshots from JP Morgan Chase for two cash withdrawals of \$10,000 in cash that occurred from JPM 8736 on March 9, 2019 and March 11, 2019 respectively. A comparison of the Adebogun's Texas driver's license photo and the JPM photo snapshots appears to demonstrate that the individual making the withdrawals from JPM 8736 is Adebogun.

28. I obtained additional information on Adebogun from other law enforcement agencies. In March 2017, the Dallas, Texas Police Department received information from Adebogun's ex-wife about possible financial fraud and identity theft being committed by Adebogun. While residing with Adebogun, the ex-wife found two passports with Adebogun's photo but the passports had different names. In addition, the ex-wife also found numerous paystubs with Adebogun's social security number but different names on the paystubs. In May

2017, FBI Special Agents in Dallas, Texas interviewed Adebogun as a follow up to his ex-wife's complaint to the Dallas Police Department. Adebogun told the FBI Special Agents he is from Nigeria and moved to the United States in 2015 on an F1 Student Visa. Adebogun at the time was not attending school and had no known employment. Adebogun provided his phone number as 682-347-2424 and his email address as adedotun_adebogun@yahoo.com to the FBI Special Agents. Adebogun denied being involved in possession of fictitious passports or identification documents.

BACKGROUND CONCERNING EMAIL

29. In my training and experience, I have learned that Oath Holdings Inc. provides a variety of on-line services, including electronic mail ("email") access, to the public. Oath Holdings Inc. (formerly Yahoo Holdings, Inc.) holds data for Yahoo namespace email accounts. Oath Holdings Inc. allows subscribers to obtain email accounts at the domain name yahoo.com, like the email account[s] listed in Attachment A. Subscribers obtain an account by registering with Oath Holdings Inc. During the registration process, Oath Holdings Inc. asks subscribers to provide basic personal information. Therefore, the computers of Oath Holdings Inc. are likely to contain stored electronic communications (including retrieved and unretrieved email for Oath Holdings Inc. subscribers) and information concerning subscribers and their use of Oath Holdings Inc. services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. In general, an email that is sent to an Oath Holdings Inc. subscriber is stored in the subscriber's "mail box" on Oath Holdings Inc. servers until the subscriber deletes the email.

30. An Oath Holdings Inc. subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, chat/messenger data, calendar data,

pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Oath Holdings Inc. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

31. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that even if subscribers insert false information to conceal their identity, I know that this information often provide clues to their identity, location or illicit activities.

32. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

33. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

34. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic

location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

35. The facts set forth in this affidavit are based on my personal knowledge, including what I have learned through my training and experience as a law enforcement officer, my review of documents and other records obtained in the course of this investigation, information I have obtained in the course of this investigation from witnesses having personal knowledge of the events and circumstances described herein, and from other law enforcement officers, all of whom I believe to be truthful and reliable.

CONCLUSION

36. Based on the facts and circumstances set forth in this affidavit, I submit that there exists probable cause to believe that the email accounts in Attachment A may contain evidence of violations of Title 18 Section 1343 (Wire Fraud), Title 18 Section 1349 (Attempt and Conspiracy), and Title 18 Sections 1956 (Money Laundering).

37. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Oath Holdings Inc. Because the warrant will be served on Oath Holdings Inc., who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with adedotun_adebogun@yahoo.com, benshak@yahoo.com, michael.john160@yahoo.com, and jazz_jassan@yahoo.com that is stored at premises owned, maintained, controlled, or operated by Oath Holdings Inc., a company headquartered at 701 First Avenue, Sunnyvale, California 94089.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Oath Holdings Inc. (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. All customer information (e.g. name, age, email address, physical address, payment information) associated with the accounts;
- b. The contents of all emails associated with the accounts from February 1, 2019 – the Present, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;
- c. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- d. The types of service utilized;
- e. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;
- f. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken
- g. Any and all methods of payment provided by the subscriber to Oath Holdings Inc. for any premium services;
- h. All records and information and analytics collected by the Provider through the use of cookies or similar technology including the type of browser and device used by the account holder, the web page visited before coming to Oath Holdings Inc. sites, and other identifiers associated with the devices used by the account holder;
- i. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Oath Holdings Inc.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence, and instrumentalities related to violations of Title 18, United States Code, Sections 1343, 1349, and 1956, those violations involving Adedotun Adebogun and occurring after February 1, 2019, including for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. Information identifying the persons using the accounts;
- b. Information identifying other accounts used by the persons using the accounts;
- c. Information identifying the devices used to access the accounts;
- d. The location of persons using the accounts;
- e. Financial information, credit card numbers, social security numbers, and other personal identifiable information;
- f. Communications made in furtherance of the fraud scheme;
- g. Communications with other individuals assisting/participating in the fraud scheme.
- h. Communications and files that contain IP addresses and username and passwords to those IP addresses;
- i. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s);
- j. The identity of the person(s) who communicated with the user ID about matters relating to an attempt or conspiracy to commit wire fraud, and money laundering, including records that help reveal their whereabouts.
- k. Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner.